14th IMEKO TC10 Workshop Technical Diagnostics
New Perspectives in Measurements, Tools and Techniques
for system's reliability, maintainability and safety
Milan, Italy, June 27-28, 2016

Diagnostics preventive evaluation, the role of IEC 61709

Giorgio Turconi[1], Jeff Jones[2]

[1] *Comitato Elettrotecnico Italiano - CEI, Milan - Italy*
[2] *Jeff Jones – University of Warwick, Coventry - United Kingdom*

***Abstract* – Complex systems need to be fault tolerant, hence diagnostics play a key role for obtaining reliability and availability objectives. Diagnostics figures need to be predicted during the design and development phase, IEC 61709 provides support in performing such a prediction allowing to calculate failure rates in different conditions and also providing failure modes for electric components.**

I. INTRODUCTION

Complex systems may have to meet severe reliability and availability objectives related to the importance of the service being provided; such systems must be fault tolerant.

In fact, fault tolerant systems are facing two different problems:

- on one hand designers make efforts to implement diagnostics to detect as many faults as possible, this would lead to built-in large diagnostics sub-systems;
- on the other hand, diagnostics itself may fail, and uncovered faults lead to highly undesired situations, this requires careful diagnostic design, so as not to worsen the entire system when the point of diminishing return is reached. [1]

This paper deals with the relationship between diagnostics and reliability/availability, and the role of IEC 61709 as an aid in performing reliability prediction of diagnostics performance.

II. RELATIONSHIP BETWEEN DIAGNOSTICS AND RELIABILITY/AVAILABILITY FOR COMPLEX SYSTEMS

The International Electrotechnical Commission (IEC) publications for coverage, availability, and maintenance concepts [2] [3], define a number of concepts in this area, considering all unwanted situations, after a failure occurs on parts devoted to operation or diagnostics.

Alarm defection:	inability to raise an alarm due to a fault in the diagnostic parts.
Down state:	a state of an item characterized either by a fault, or by a possible inability to perform a required function during preventive maintenance.
False alarm:	a fault indicated by built-in test equipment or other monitoring circuitry where no functional fault exists.
Fault mode:	one of the possible states of a faulty item, for a given required function.
Fault coverage:	the proportion of faults of an item that can be recognized under given conditions.
Fault diagnosis:	actions taken for fault recognition, fault localization and cause identification.
Latent fault:	an existing fault that has not yet been recognized.
Up state:	a state of an item characterized by the fact that it can perform a required function, assuming that the external resources, if required, are provided.

Usually reliability/availability is generically referred to *failures*, but only *failure modes*, i.e. the way a component, equipment or sub-system fails are relevant in order to properly address the consequence of failures.

There may exist component failure modes that do not affect a specific circuit, and there may be other failure modes that totally destroy system operation. Knowledge of failure modes and their probability of occurrence plays an important role, since diagnostics is interested in detecting *failure modes*, since their consequence affect the ability of the system to recover, i.e. to perform as a fault tolerant system, as designed.

III. PREDICTING DIAGNOSTICS PERFORMANCE

Like any reliability/availability related characteristic, diagnostics need to be predicted during the design and development phase, and then tested.

Diagnostics prediction includes calculation of related figures: fault coverage, as a main parameter, and probability of occurrence of any other failure mode's related system state [1].

To do that component failure modes are needed and IEC 61709 helps to provide this data.

The characteristic preferred for reliability data of electric components is the failure rate. It is to be noted that, although it is often generically defined as failure, the exact observed event that is measured is a *failure mode* and in equipment a failure or functional loss is caused by

a component failure where component failure mode is relevant to the application being carried out by the equipment.

It should be noted that a component has many features and only some may be used in the specific circuit or application. A function loss at the equipment level occurs only when there is a loss of the component feature that is used to support that function.

A circuit requires the presence of component features according to what was defined by the designer; this may not encompass the total feature set of the component and may not use a particular feature to its full capacity as defined by the data sheet in terms of functional characteristics and ratings.

Handbooks usually define failure rate, assumed to be constant, as an overall value, which includes all failure modes. This implies that component failure rate can be considered as the sum of the failure rates of all the modes, as follows:

$$\lambda_{\text{comp}} = \sum_{i=1}^{n} (\lambda_{\text{m}})_i \qquad (1)$$

where λ_{comp} is the component failure rate in which the failure mode $(\lambda_{\text{m}})_i$ occurs and n is the number of failure modes.

Failure modes for electric components are provided by IEC 61709. Once relevant failure modes are identified, it is possible to calculate diagnostics figures.

Reliability models involve some simplifications. In a block diagram each functional block has two states: one state means correct operation (*up state*) and the other means fault (*down state*). This two-state model greatly simplifies reliability analysis, but in fact each block of a fault tolerant system contains circuits devoted to perform the functional features and circuits devoted to diagnostics. What happens when circuits devoted to diagnostics fail? In other terms, what happens when a fault is *not covered* by diagnostics?

Since (Fault) Coverage is the proportion of recognized faults, we can define $\lambda_{F/C}$ as the covered failure rate of the functional circuit (failures detectable by diagnostics), and $\lambda_{F/NC}$ as the uncovered failure rate. Considering λ_F the total failure rate of the circuit, it follows that

$$\lambda_F = \lambda_{F/C} + \lambda_{F/NC} \qquad (2)$$

Coverage is then

$$C = \frac{\lambda_{F/C}}{\lambda_{F/C} + \lambda_{F/NC}} \qquad (3)$$

Uncovered failures will lead, depending on the failure mode as perceived by the circuits to false alarm or alarm defection, thus affecting the designed characteristics of diagnostics.

IV. THE ROLE OF IEC 61709

Reliability prediction is one of the oldest and most common reliability methodologies and often affects major decisions in system design.

It is based on the assumption that systems fail as a result of failures of component parts, and those parts fail partly as a result of exposure to application stress [4]. This means that by some consideration of the structure of such a piece of equipment and by further consideration of its usage it is possible to obtain an estimate of the systems reliability in that particular application.

There are many reasons why this task may be necessary. These include feasibility evaluation where the compatibility of a design concept is weighed against the design reliability requirements for acceptance, and design comparison where different parts of a system can be compared and any necessary trade-off such as cost, reliability, weight etc. can be made.

Further uses are for the identification of potential reliability problems and as a reliability input into other tasks such as maintainability analysis, testability evaluations and FMECA [5].

Rightly or wrongly reliability prediction methods are widely accepted throughout the engineering industry and these methods are often used as a yardstick for the comparison of different equipment.

However, many manufacturers have commented that the models can be wildly inaccurate when compared with the performance in the field, particularly in the case of the observed failure rates of modern microelectronic devices, and their use can lead to increased costs and complexity while deluding engineers into following a flawed set of perceptions and leaving truly effective reliability improvement measures unrecognized [4].

IEC 61709 [6] is intended to support the reliability prediction process and gives guidance on stating and using failure rate data for components used in equipment.

Reference conditions for failure rate data are specified, so that data from different sources can be compared on a uniform basis and the standard also provides acceleration models for conversion of failure rate data from reference conditions to operating conditions including a method for dealing with missions that have multiple phased operating conditions.

IEC 61709 does not, of course, contain any failure rate data, it is not the task of a standardization body to collect, analysis and provide such data, rather IEC 61709 provides the means for working with existing data be it from field data collection, manufacturers data or from reliability handbooks and the standard does provide a list of handbook data sources.

In fact many of the acceleration formulae contained in the standard were derived by consideration of the different handbook reliability models and in many case are an empirical fit to data points generated from the different handbook procedures.

V. PHILOSOPHY OF IEC 61709

IEC 61709's basic philosophy is based around a

component model that considered a component to consist of the actual component itself (e.g. silicon die), the encapsulation (e.g. case) and connection points. How the connection points are attached to the circuit board, also called the attachment system (e.g. solder joint), are treated separately.

The component then has a failure rate, defined under reference conditions, that is related to the physics of failure of the device.

Table 1. IEC 61709 Reference conditions.

Type of stress	Reference condition
Ambient temperature(1)	θ_0 = 40 °C
Environmental condition	Stationary use at weather-protected locations The environment is highly insensitive to the weather outdoors and humidity is controlled within defined limits. This is typical of telecommunications and computer equipment placed in buildings. This includes office situations.
(1) The ambient temperature for the purpose of this standard is the temperature of the medium next to the component during equipment operation, not taking into account any possible self-heating of the component. The surroundings of the component should be defined.	

Table 2. Example of reference conditions.
Transistors common, low frequency.

Component	Ref. temp. °C	Ref. voltage ratio
Bipolar, universal e.g. TO18, TO92, SOT(D)(3)23 or similar	55	$U_{ref}/U_{rat} = 0{,}5$
Transistor arrays	55	
Bipolar, low power e.g. TO5, TO39, SOT223, SO8, SMA-SMC	85	
Bipolar, power e.g. TO3, TO220, D(D)-Pack	100	
FETjunction MOS	55 55	
MOS power (SIPMOS) e.g. TO3, TO220, D(D)-Pack	100	

Each device type has a number of mechanisms that contribute to this failure rate and these are triggered by different activation energies and will have a reaction rate dependent on the appropriate stress applied to the component. This means that each component type has a specify set of stress models that describes how the failure rate changes when the appropriate stress (or set of stresses) is applied.

These stress models provide an acceleration factor that can be then used to predict how the component may behave under different conditions.

Each failure rate model has been derived from a consideration of the device physics or by empirical curve fitting to available data and so in both cases provides a good and realistic approximation of reality.

For example, the thermal design of a system is considered by most component type supported as one of the main stresses affecting reliability. This thermal effect is based around a consideration of junction temperatures and how they are affected by the thermal geography of a system. IEC 61709 provides procedures that allow the junction temperature of any relevant device to be estimated based on systems ambient temperatures and from this junction temperate estimate failure rates can be derived using the procedures contained in the standard.

By combing the failure rates at different stress levels through a mission model and by summing up the resulting failure rates for all components in a system it is possible to perform a parts stress prediction for a system in a manner similar to that supported by MIL-HDBK 217 [7].

In order to better support a prediction approach, the standard provides the likely ration of failure modes for many component types where possible and also provides for many life-limited component types methods of estimating useful lifetime during which the methodology supported by the standard applies.

Table 3. Example of IEC 61709 failure modes.
Transistor, diode, optocoupler

		Short circuit %	Open circuit %	Drift %	Forward leakage current drift %
Transistors	Silicon	85	15		-
	GaAs	95	5		-
Diodes	Silicon	80	20		-
	GaAs	95	5		-
Zener diodes		70	20	10	
Thyristors		20	20		60
Optocouplers		10	50	40	-
Laser diodes		85	15	-	-

VI. OWNERSHIP OF FAILURE RATES

As already mentioned the standard does not provide any failure rate data, rather it describes a methodology for using such data and although it is possible to use handbook data or manufacturers data with the procedures described it is much better for a user if they use their own data.

To this end the standard contains some information on how a database to hold this data should be designed and together with IEC 60300-3-2 [8] provides sufficient information of an organization to set up a data collection and storage systems to work with the models contained with this standard.

VII. TESTING AND ANALYSIS

Every failure has its own cause. Considering failures as random is a conventional way to describe all those cases in which it is impossible or too expensive to search or identify the causes, even if it is known this is the only way to avoid their occurrence.

The possibility of identifying the failure causes (excluding failures due to external causes) depends on the capacity of testing and analysis tools (instruments, resources, know-how).

To what extent should causes of a failure be sought?

Failures have a cost (including either repair costs or induced costs on users and on offered services, including loss of market share), and physical analysis has a cost, so the break-even point is found by balancing these two costs, nevertheless efforts toward physical failure analysis cannot be avoided, being this the only available method toward improvement.

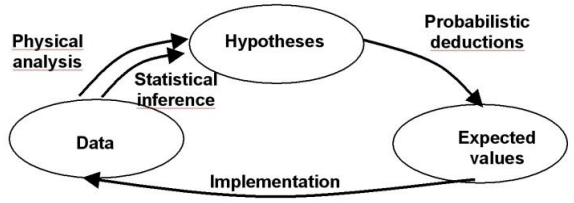

Fig. 1. The reliability method.

Figure 1 shows the reliability method, which requires feedback between prediction and realization, an iterative process where measurements play a fundamental role in success.

In fact reliability engineering is aimed to improvement, hence feedback between expected data and real field data cannot be limited to statistical inference, since efforts need to be made to fix possible mistakes and flaws originated by design, manufacturing, installation, operation, and maintenance.

Only (physical) failure analysis can help to perform this task, prediction models having to be based on the best practices, i.e. the best reliability performance obtained in the field.

VIII. CONCLUSIONS

Fault tolerant systems, where diagnostics play an important role, require that diagnostics reliability performance be evaluated. IEC 61709 helps in performing this task providing models for converting failure data among different conditions and also providing component failure modes, necessary to properly evaluate diagnostics reliability performance at prediction level.

IX. REFERENCES

[1] G. Turconi, E. Di Perna, "A Design Tool For Fault Tolerant Systems", IEEE RAMS, January 2000, Los Angeles, pp 317-326

[2] IEC 706-2 (1990) Guide on maintainability of equipment Part 2: Section five: Maintainability studies during the design phase.

[3] IEC 706-5 (1994) Part 5: Section 4: Diagnostic testing.

[4] C. T. Leonard and M. Pecht, "How failure prediction methodology affect electronic equipment design", Quality and Reliability Engineering International, Vol. 6, 1990, pp 243-249.

[5] B. S. F. Morris, "Use and application of MIL-HDBK-217", Solid State Technology, August 1990, pp 65-69.

[6] IEC 61709, Electric components – Reliability – Reference conditions for failure rates and stress models for conversion.

[7] US MIL-HDBK-217,"Reliability Prediction of Electronic Equipment", Version F, Dec. 1991.

[8] IEC 60300-3-2, Dependability management - Part 3-2: Application guide - Collection of dependability data from the field.